International Journal of Computer Applications (0975 - 8887)
Volume 186 - No.42 , September 2024

Notes on ”On the Design of a Privacy-preserving Communication Scheme for Cloud-based Digital twin Environments using Blockchain”

Fauzia Hassan
School of Basic and Applied Sciences,
Shobhit Institute of Engineering and Technology
Meerut, Uttar Pradesh - 250110, India

Vinod Kumar
Department of Mathematics, Shyam Lal College
University of Delhi
New Delhi-110032, India

Anil Kumar Nishad
School of Basic Science
Galgotias University
Greater Noida, Uttar Pradesh- 203201, India

Adesh Kumari
Department of Mathematics
Jamia Millia Islamia
New Delhi-110025, India

ABSTRACT

The innovative paradigm of Digital Twin (DT) technology is transforming our understanding of DT and interactions with the physical environment. It entails building DTs, or virtual replicas, that precisely imitate the traits, actions, and features of actual systems, processes, or things. These dynamic DTs provide continuous, bidirectional communication between digital and physical domains while changing in real time. DT is a multi-physical, multi-scale, and multi-dimensional technology. At the same time, it is characterized by real-time synchronisation, realistic mapping, and high fidelity. It allows the physical world and the information world to see connection and integration between the physical and information worlds. In recent years, DT technology has attracted the attention of academic professionals, especially its applications. When it comes to the world of the internet, security and privacy are of major concern. In the proposed paper, we have reviewed a mutual authentication scheme proposed by Son et al.'s [1] and cryptanalysed the scheme in order to get an idea in which direction further work has to be done. We show that the proposed scheme fails to prevent insider attacks, stolen smart card attacks, known session-specific temporary information attacks, and lack of mutual authentication. Additionally, we propose several enhancements within the same framework.

Keywords

Digital Twin, Security and Privacy, Mutual Authentication, Security attacks

1. INTRODUCTION

The use of DT technology has revolutionized the design, monitoring, and optimization of complex systems, revolutionising manufacturing, industry, and other domains [2]. DTs, which have their roots in the meeting point of the real and virtual worlds, are digital copies or counterparts of physical objects, such as systems, products, processes, or even entire ecosystems. These innovative ideas are transforming industries by providing heretofore unseen information, improved decision-making processes, and better performance over the lifecycle of companies [3].
Internet of Things (IoT) devices use sensors and other data sources to constantly update their dynamic, real-time physical counterpart, known as DT. This twin is not the current state of a physical object but also simulates its behavior under different conditions, allowing for decision-making and predictive analytics technology that uses advanced analytics, artificial intelligence (AI), and communication to bridge the gap between the physical and digital world networks, enabling efficiency, responsiveness, and innovation [4].

1.1 DIFFERENT SORTS OF DTs:

Different sorts of DTs exist, depending on their use, complexity, and range [5]. Fig. 1 shows different sorts of DT, and below we provide a description of them:

—**Component Twin:** A basic DT is the digital fabrication of a physical component, such as a circuit board, sensor, or bearing. Component twins can be used to predict when a component is likely to disconnect and are often used to test the overall performance and compatibility of character connectors.

—**Product Twin:** A digital replica of an actual product, like an engine, wind turbine, or plane, is regularly known as an asset twin. Compared to component twins, these are extra complicated and may encompass aspects of the conduct, structure, and capability of the product. Product twins may be used to expect product screw-ups, enhance upkeep, and optimize product design, among other things.

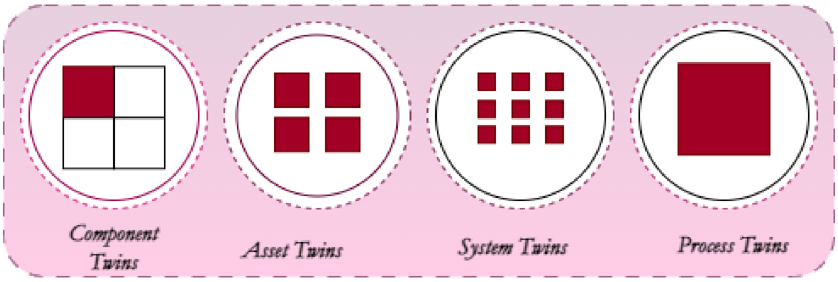

Fig. 1. Sorts of DT

—**System Twin** An automated duplicate of a complicated device, like a metropolis, manufacturing facility, or electricity grid, is referred to as a system twin. The most elaborate kind of DTs are known as system twins, and they could contain fashions of the environment, interactions, and elements of the device. System simulation, operational optimization, and the detection of possible device breakdowns are only a few of the numerous uses for system twins.

—**Process Twin:** A digital reproduction of a physical system, like a delivery chain, chemical response, or industrial process, is referred to as a process twin. Physical strategies can be modeled, determined, and optimized using procedure twins. Process twins can be applied to decrease waste, find possible problems, and improve growth procedure performance.

1.2 USE OF DT IN DIFFERENT SECTORS

Many industries use DT, including manufacturing, healthcare, energy, transportation, and concrete placement. For example, manufacturing DT can be used to predict maintenance needs in manufacturing, track appropriate equipment, and improve surgical success. DT provides insight into specific clinical issues and treatment outcomes, enabling customized predictive interventions in the healthcare industry. DT generation is being used in ecosystems and complex systems, not just for men and women. Smarter city-making plans and management may be facilitated, for example, with the aid of the use of DTs in cities to duplicate site visitor patterns, environmental conditions, and concrete infrastructure. Because of its adaptability, this era is a chief facilitator of Industry 4.0 and the IoT, selling sustainability, performance, and creativity [6]. Apart from these sectors, many other fields propose the idea of adapting DT such as agriculture, architecture [7], and many more.
But enforcing the DT era has its own set of difficulties, including the requirement for mounted protocols for interoperability, cybersecurity risks, and other safety troubles. The benefits of DTs in terms of lower prices, greater effective operations, and higher decision support are encouraging extra attention and funding as corporations manage these problems.

1.3 LITERATURE REVIEW

The idea of twinning was first presented by NASA in the 1960s for their Apollo programme, which aimed to build physical replicas of their systems in space on Earth. This is when the DT concept first emerged. The concept enabled them to test numerous cases and conditions, simulate various scenarios and evaluate the behaviour of their systems execution. It gained additional attraction when the twin saved the day after experts on Earth tested potential fixes on the ground twin in order to remedy technical issues encountered during the Apollo 13 mission [8]. Michael Grieves, however, did not develop the idea of DTs for the industrial sector until the early 2000s. He did this by building virtual factories that could be used to track operations, anticipate malfunctions and boost output [9]. The concept became more popular and important after it was added by Gartner in their list of the top 10 strategic technology trends of 2017 [10] and embraced by a number of major corporations and General Electric [11]. DT is a digital representation of the physical system and its ongoing operation that is established through data communication and provides the transition from the physical system to the virtual system while maintaining a high level of connectivity between them. The primary distinction between DTs and digital models/shadows of systems, as emphasised by the authors of [12], is the type and direction of data flow that occurs between real and virtual systems. Unlike digital images or shadows, which do not have a complete data integration cycle, DTs have an actual data flow that integrates in both directions between physical and digital systems to give the digital object its original matching of the current ground state and also sends control information to it. This has also been emphasised in [13] and [14], where the connection between digital and physical systems that transfers data and control information between them was described as the key component of DTs. The ideal goal for DTs is to provide all necessary information about the physical system in real-time [13].

1.4 MOTIVATION AND CONTRIBUTION

The security of online transactions and data transfers is crucial in the quickly changing world of digital communication and information exchange. Mutual authentication systems are essential for guaranteeing the security and integrity of sensitive data that is shared between parties in a variety of applications, including secure communication protocols, online banking and e-commerce.
Our research applies cryptanalysis to mutual authentication scheme proposed by Son et al. with the goal of making a major contribution to the field of cryptographic security. Among the main contributions of our work are:

—We reviewed scheme proposed by Son et al.

—We find that their scheme cannot stand with various security attacks, such as:

  —Offline password getting attacks
  —Known session-specific temporary information attack
  —No mutual authentication
  —Smart card stolen attack
  —User anonymity

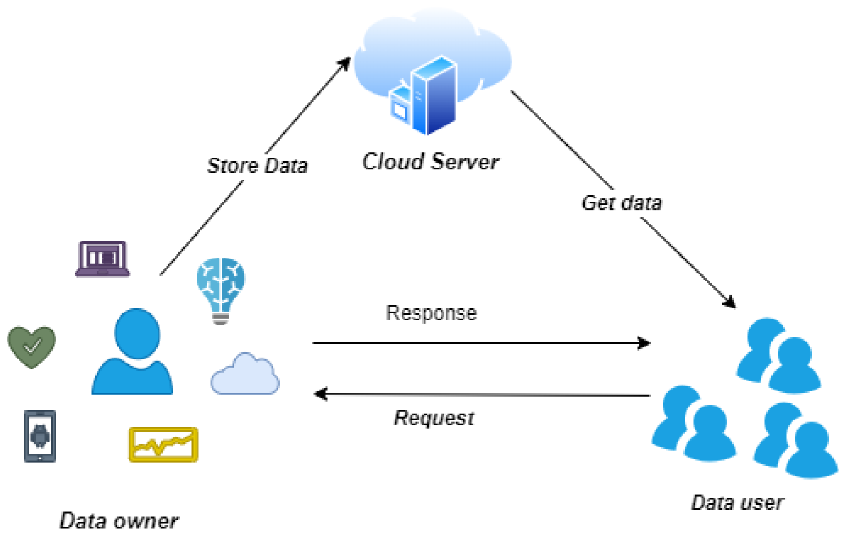

Fig. 2. System model

1.5 ROADMAP OF THE PAPER

This paper includes 5 sections. In Section 2, scheme for security of DT proposed by Son et al. have been discussed. In Section 3, we have done the cryptanalysis of scheme. In Section 4, we suggest some improvements for the discussed schemes. Finally, we have presented our conclusion and future direction in section 5.

2. REVIEW OF SON ET AL.' SCHEME

In this section, we have shown the scheme proposed by Son et al. Although their scheme claim to be very helpful and secure against various attacks, we have made an effort to show that they do not offer high security. Fig 2 depicts the system model used by Son. Below are the details of the schemes. First, we will go through the whole process involved in the scheme. The notation used in the scheme is described in Table 1.

2.1 INITIALIZATION PHASE

In this phase, TA chooses a non-singular elliptic curve $E_q(c,d)$: $y^2 = x^3 + cb + d \ mod \ q$ over F_q where $4c^3 + 27d^2 \ mod \ q \neq 0$ where q is a large prime. To compute the public key P_{TA}, TA chooses a base point P on $E_q(c,d)$, K_{TA} (the secret key) and computes $P_{TA} = K_{TA}.P$. Further, TA chooses two multiplicative groups, namely G and G_t, two cryptographic hash functions. And publishes the system parameters $\{G_t, G, P_{TA}, P\}$.

2.2 REGISTRATION PHASE

To participate in the network, every entity that is involved in this protocol has to get registered with TA during the registration phase.

Step 1. Firstly, TA chooses ID_m, r_m and computes $P_m = r_m.P$, where the r_m denotes the private key for S_m.

Step 2. By utilizing D_k, O_k registers itself with TA. O_k chooses its ID_k, PW_k also selects a random nonce, i.e. $g_k \in Z_q$. Finally, O_k computes $HID_k = H(ID_k \| PW_k \| g_k)$ and sends $\{ID_k, \ HID_k\}$ to TA.

Step 3. TA generates r_k after receiving the message and computes SID_k, which is equivalent to $SID_k = r_k.HID_k$ and sends $SID_k = r_k.HID_k$ to O_k.

Step 4. Finally, on receiving the message, O_k computes $HPW_k = h(ID_k \| PW_k)$, $A_k = g_k \oplus HPW_k$ and $C_k = r_k \oplus h(g_k \| HPW_k)$, $E_k = SID_k \oplus h(r_k \| g_k \| HPW_k)$ and $Auth_k = h(r_k \| g_k \| SID_k)(modn)$. Finally, O_k stores $\{A_k, C_k, E_k, Auth_k, n\}$ in D_k.

2.3 AUTHENTICATION PHASE OF CLOUD-OWNER

To transfer the data collected by the physical assets, authentication is required. The steps involved in the authentication process of O_k and S_m with each other are listed in Table 2:

2.4 AUTHENTICATION PHASE OF USER-OWNER

U_l can request O_k for the DT data when required. The authentication process of U_l and O_k with each other is done in Table 3;

3. CRYPTANALYSIS OF SON ET AL. WORK

In this section, we made an effort to cryptanalyze the scheme presented by Son et al. and prove that it is not sufficient to provide better security.

3.1 INSIDER ATTACK

Let's assume that any $\mathcal{A}$ is an insider from TA, he will have to guess the PW_k of O_k. Suppose $\mathcal{A}$ guesses the password as PW_k^* and computes $HID_k = h(ID_k \| \ PW_k^* \| \ g_k)$. If $HID_k^* \stackrel{?}{=} HID_k$, then it is easy for any attacker to get access. That means that the proposed framework is not resilient to insider attacks.

3.2 SMART CARD STOLEN ATTACK

The owner's smart device, that is, D_k is the most valuable asset. Suppose that if any adversary $\mathcal{A}$ steals D_k he can have access to various hidden parameters such as ID_k, HID_k. With the help of

Table 1. Notations

Symbol	Description	Symbol	Description
O_k	k_{th} Data owner	ID_k	Identity of O_k
SID_k	Secret identity of O_k	PW_k	Password of O_k
S_m	m_{th} cloud server	U_l	l_{th} data user
TA	Trusted authority	$u_l,\ u_k$	Random nonce
$b_l,\ b_k$	Secret key of $U_l,\ O_k$	$L_l,\ L_k$	Message digest of $U_l,\ O_k$
Req	Request message of U_l	SK	Session key
$\|$	The concatenation operator	$\oplus$	Bitwise XOR operation
$\Rightarrow$	Secure channel	$\rightarrow$	Public channel

Table 2. Authentication phase between O_k and S_m

O_k	S_m
Inputs PW_k^* and ID_k^*	
Computes $HPW_k = h(PW_k \| ID_k)$	
$g_k = A_k \oplus HPW_k$	
$r_k = C_k \oplus h(HPW_k \| g_k)$	
$SID_k = E_k \oplus h(r_k \| g_k \| HPW_k)$	
Checks $Auth_k \stackrel{?}{=} h(r_k \| g_k \| SID_k)(modn)$	
Generates $c_k \in Z_q^*, T_1$	
Computes $HID_k = H(ID_k \| PW_k \| g_k)$	
$R_k = r_k.g_k.P$	
$R_{km} = c_k.g_k.P_m$	
$PID_k = HID_k \oplus h(r_{km} \| T_1)$	
$X_k = SID_k.h(HID_k \| r_{km} \| T_1)$	Checks if $\|T_1 - T_1^*\| \leq \Delta T$
Sends $\{R_k, PID_k, X_k, T_1\}$	Computes $R_{km} = r_m.R_k$
$\cdots\cdots\cdots\rightarrow$	$HID_k = PID_k \oplus h(R_{km} \| T_1)$
	Checks $\bar{e}(X_i, P) \stackrel{?}{=} \bar{e}(HID_i.h(HID_i \| R_{ij} \| T_1), P_{TA})$
	Generates $r_m \in Z_p^*$ and T_2
	Computes $R_{mk} = r_k * R_m$
	$SK_{mk} = h(R_{mk} \| R_{km} \| HID_k$
	$L_m^* \stackrel{?}{=} h(SK_{mk} \| R_{mk} \| R_{km} \| T_2)$
	Sends $\{R_m, L_m, T_2\}$
Checks if $\|T_2 - T_2^*\| \leq \Delta T$	$\leftarrow\cdots\cdots\cdots$
If valid, computes $R_{mk} = c_k.g_k.R_m$	
$SK_{km} = h(R_{km} \| R_{mk} \| HID_k)$	

smart card stolen attack, $\mathcal{A}$ can guess the password in following ways:
Suppose $\mathcal{A}$ guesses the password PW_k^* and tries to compute $HPW_k^* = h(ID_k \| PW_k^*)$. Next, E calculates $a_k^* = A_k \oplus\ HPW_k^*$ and $HID_k^* = H(ID_k \| PW_k^* \| a_k^*)$. $HID_k^* \stackrel{?}{=}\ HID_k$ holds. This shows that the proposed framework is not resilient to stolen smart device attacks.

3.3 KNOWN SESSION-SPECIFIC TEMPORARY INFORMATION ATTACK (KSSTIA)

In this attack, it is believed that u_l and u_k are known to $\mathcal{A}$, that is, the random nonces. In order to compute the session key, some parameters like $U_{kl},\ U_{lk},\ HID_l$ and HID_k must be known to $\mathcal{A}$. Therefore, $\mathcal{A}$ computes $U_{kl} = u_k.X_l,\ HID_k = H(ID_k \|\ PW_k \|\ g_k)$. By above mentioned privileged insider attack, r_k is known to E and therefore he can compute $SK_{lk} = Q_l.r_k, HID_l = PID_l \oplus\ h(U_{lk} \| T_3)$ i.e, $SK_{kl} = h(U_{lk} \| U_{kl} \| HID_l \| HID_k)$ can be computed. Thus, the proposed protocol is vulnerable to KSSTIA.

3.4 NO MUTUAL AUTHENTICATION

The O_k initially confirms the time stamp standards as $|T_3 - T_3^*| \leq \Delta T$. After receiving the records request message from U_{lk} as $U_{lk} =\ r_l.Q_l$, O_k no longer has access to the person's non-public key as U_{lk} makes use of the user's private key, r_l, that which is produced through TA. Thus, this illustrates the protocol's design problem.

3.5 USER ANONYMITY

Anonymity and identity protection allow the user to hide their identifying information online. In the proposed scheme, they did not use an anonymous form. This gives any $\mathcal{A}$ the opportunity to track all of the authenticated users. Hence, the proposed scheme fails to ensure user anonymity.

4. SUGGESTED IMPROVEMENTS FOR SON ET AL.'S SCHEME

In order to handle new difficulties, Son et al.'s scheme would benefit from continued development and evolution through collaboration with the research community. There are some improvements that can be made to the scheme, like:

Table 3. Authentication phase between U_l and O_k

U_l	O_k
Generates Req_l, u_l, T_3	
Computes $U_l = u_l.g_l.P$	
$U_{lk} = u_l.g_l.P_k$	
$PID_l = HID_l \oplus h(U_{lk} \| T_3)$	
$M_l = Req_l \oplus h(HID_l \| U_{lk} \| T_3)$	
$X_l = SID_l.h(HID_l \| Req_l \| U_{lk} \| T_3)$	
Sends $\{Q_l, PID_l, M_l, X_l, T_3\}$	
$\cdots\cdots\cdots \rightarrow$	
	Verifies $\lvert T_3 - T_3^* \rvert \leq \Delta T$
	Computes $U_{lk} = r_l.Q_l$
	$HID_l = PID_l \oplus h(U_{lk} \| T_3)$
	$Req_l = M_l \oplus h(HID_l \| U_{lk} \| T_3)$
	Checks $\bar{e}(X_i, P) \stackrel{?}{=} \bar{e}(HID_i.H(HID_i \| Req_i \| U_{lk} \| T_3), P_{TA})$
	Generates $u_k \in Z_p, T_4$
	Computes $U_k = u_k.P$
	$U_{kl} = u_k.X_l$
	$SK_{kl} = h(U_{kl} \| U_{lk} \| HID_l \| HID_k)$
	Verifies $L_k \stackrel{?}{=} h(SK_{kl} \| U_{lk} \| U_{kl} \| T_4)$
	Sends $\{U_k, L_k, T_4\}$
	$\leftarrow \cdots\cdots\cdots$
Checks $\lvert T_4 - T_4^* \rvert \leq \Delta T$	
Computes $U_{kl} = u_k.X_k$	
Computes $SK_{kl} = h(U_{lk} \| U_{kl} \| HID_l \| HID_k)$	
Checks $L_k \stackrel{?}{=} h(SK_{kl} \| U_{lk} \| U_{kl} \| T_4)$	

—Password update is required in the Son et al. scheme.

—A biometric approach can be used, which is very difficult to break for any $\mathcal{A}$.

—Using the biometric approach, even while using the stolen smart card, $\mathcal{A}$ will have to calculate the passwords of O_k which can be avoided using biometric information in the passwords.

—Apply the proper blockchain methods in the twin system.

5. CONCLUSION AND FUTURE SCOPE

The DT era has emerged as one of the most promising innovations in diverse industries, imparting brilliant capability to change the manner in which merchandise and techniques are manufactured, processed, and managed. For instance, manufacturers can use DT to create realistic physical models, permitting them to simulate and assume manufacturing behaviour underneath real-world situations. This functionality isn't that it offers no longer the simplest simplifies manufacturing techniques, but additionally improves overall performance control and predictive protection. In healthcare, DT may be used to create digital images of sufferers, permitting their fitness records to be tracked and analysed over the years. This technique facilitates individualised treatment planning and improves conventional treatment effectiveness. By constantly tracking and mapping affected person situations, health care organisations can, because it should count on health effects and interfere aggressively while needed. As the use of DT generation continues to increase, the importance of making sure stringent safety measures will grow. With DTs appearing as particular virtual replicas of physical items, any breach or manipulation of this data has to pose massive risks, specifically in sensitive regions inclusive of healthcare, areas, infrastructure, and plenty of others. This paper demonstrates how Son's plan is vulnerable to several security flaws and insufficient security. Using this paper, one can identify the potential areas for improvement and opportunities to apply the analysis to modern encryption systems. Furthermore, this paper will help new researchers in broader security research develop stronger cryptographic protocols or improve the understanding of cryptographic vulnerabilities in evolving systems.

6. REFERENCES

[1] Seunghwan Son, Deokkyu Kwon, Joonyoung Lee, Sungjin Yu, Nam-Su Jho, and Youngho Park. On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain. *IEEE Access*, 10:75365–75375, 2022.

[2] Fauzia Hassan, Vinod Kumar, Anil Kumar Nishad, and Vinay Gautam. Investigation of digital twin technology for secure and privacy preserving networking. *Procedia Computer Science*, 230:398–406, 2023.

[3] Diego M Botín-Sanabria, Adriana-Simona Mihaita, Rodrigo E Peimbert-García, Mauricio A Ramírez-Moreno, Ricardo A Ramírez-Mendoza, and Jorge de J Lozoya-Santos. Digital twin technology challenges and applications: A comprehensive review. *Remote Sensing*, 14(6):1335, 2022.

[4] Fei Tao, Bin Xiao, Qinglin Qi, Jiangfeng Cheng, and Ping Ji. Digital twin modeling. *Journal of Manufacturing Systems*, 64:372–389, 2022.

[5] Mengnan Liu, Shuiliang Fang, Huiyue Dong, and Cunzhi Xu. Review of digital twin about concepts, technologies, and industrial applications. *Journal of manufacturing systems*, 58:346–361, 2021.

[6] Deuk-Young Jeong, Myung-Sun Baek, Tae-Beom Lim, Yong-Woon Kim, Se-Han Kim, Yong-Tae Lee, Woo-Sug Jung, and In-Bok Lee. Digital twin: technology evolution stages and im-

plementation layers with technology elements. *IEEE Access*, 10:52609–52620, 2022.

[7] Qamar Irshad and Zaheer Abidi. Outpatient department in hospitals: A critical analysis. 2020.

[8] Peter Augustine. The industry use cases for the digital twin idea. In *Advances in Computers*, volume 117, pages 79–105. Elsevier, 2020.

[9] Michael Grieves and John Vickers. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. *Transdisciplinary perspectives on complex systems: New findings and approaches*, pages 85–113, 2017.

[10] B Burke, M Walker, and D Cearley. Top 10 strategic technology tends for 2017. *14th October*, 2016.

[11] Qinglin Qi, Fei Tao, Tianliang Hu, Nabil Anwer, Ang Liu, Yongli Wei, Lihui Wang, and AYC Nee. Enabling technologies and tools for digital twin. *Journal of Manufacturing Systems*, 58:3–21, 2021.

[12] Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow. Digital twin: Enabling technologies, challenges and open research. *IEEE access*, 8:108952–108971, 2020.

[13] Michael Grieves. Digital twin: Manufacturing excellence through virtual factory replication. white paper, 2014. *Online:-03-01*.

[14] Fei Tao, Jiangfeng Cheng, Qinglin Qi, Meng Zhang, He Zhang, and Fangyuan Sui. Digital twin-driven product design, manufacturing and service with big data. *The International Journal of Advanced Manufacturing Technology*, 94:3563–3576, 2018.